(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年1 月3 日 (03.01.2002)

PCT

(10) 国際公開番号
WO 02/01533 A1

(51) 国際特許分類[7]: G08G 1/137, H04M 11/00, 3/42, G06F 13/00, 17/60

(21) 国際出願番号: PCT/JP01/05664

(22) 国際出願日: 2001 年6 月29 日 (29.06.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2000-201462 2000 年6 月29 日 (29.06.2000) JP
特願2001-188724 2001 年6 月21 日 (21.06.2001) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 池田清和 (IKEDA, Kiyokazu) [JP/JP]; 〒141-0001 東京都品川区北品川6丁目7番35号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 弁理士 松隈秀盛(MATSUKUMA, Hidemori); 〒160-0023 東京都新宿区西新宿1丁目8番1号 新宿ビル Tokyo (JP).

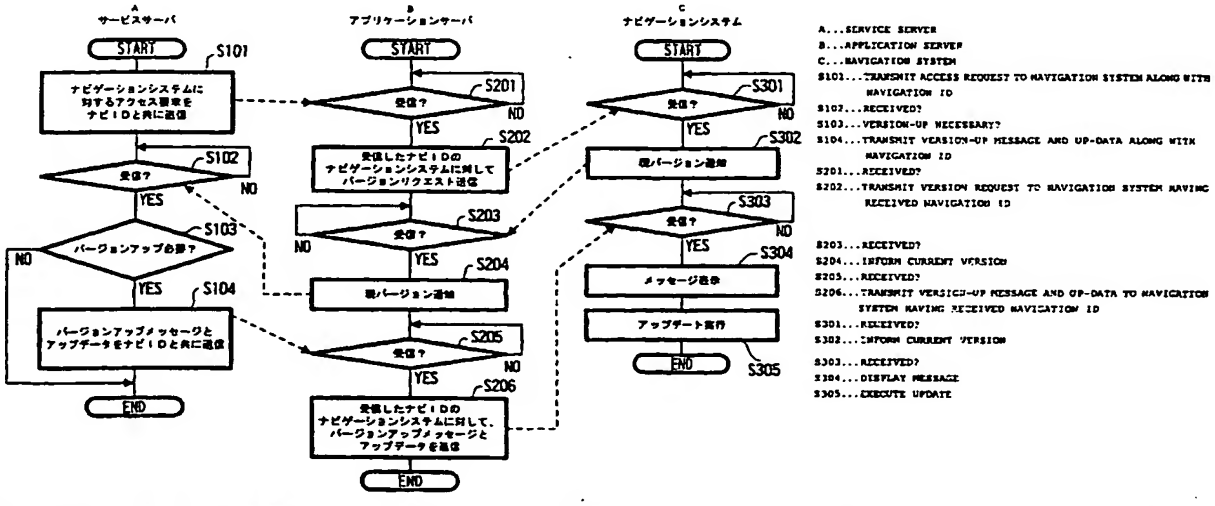
(81) 指定国 (国内): CN, DE, US.

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: SERVICE PROVIDING SYSTEM

(54) 発明の名称: サービス提供システム



(57) Abstract: A service server for providing service which uses, in order to improve after service for products purchased by users, an apparatus ID specifically allocated to a navigation system, a product purchased by a user, to access a specific navigation system and transmit navigation information. Namely, it positively accesses a navigation system that is one of an unspecified number of terminal devices on a communication network to transmit and provide service information, whereby it is possible to provide service having necessary and sufficient contents at any proper opportunity.

[続葉有]

WO 02/01533 A1

明 細 書

サービス提供システム

技術分野

本発明は、例えば自動車などの移動体に搭載される電子機器と、サーバ及び携帯電話などの個人移動端末装置とを通信網を介して通信可能なように構築されたシステムとして、例えば電子機器を購入して利用しているユーザに対して、送信されたデータを受信した電子機器が、その受信データの内容に従って何らかの動作の実行を行うことで享受できるようなサービスを提供することのできるシステムに関するものである。

背景技術

いわゆるカーナビゲーション装置が広く普及している。その基本的な機能としては、例えば移動中にある自動車などの現在位置を測定して、その測定された現在位置を地図上に表示させるなどして、ユーザに現在位置を知らせるものである。

また、近年においては、移動無線端末装置を備えることで、インターネットに接続可能な機能を有するカーナビゲーション装置も普及してきている。その利用形態としては、例えばインターネット上のＷｅｂサイトにアクセスすることで、例えば、或る特定地域の店舗の情報や、イベント、天気の情報などをカーナビゲーション装置の表示部位に表示させ、これらの情報を得ることが可能になるものである。

ところで、例えば商品を購入したユーザには、いわゆるアフターケア、アフターサービスなどといわれる、商品を購入したユーザにとって有用となるようなサービスを、その商品を製造販売したメーカや店舗から提供することがしばしば行われる。

ここで上記したようなカーナビゲーション装置もまた、元は商

テムについて以下のように構成する。

本発明のサービス提供システムは、少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器ＩＤが割り与えられる電子機器と、所定のサービス提供機能を有すると共に、サービス提供可能な複数の上記電子機器についての上記機器ＩＤが格納されるサービス用サーバと、通信網とを備えて成る。

そして、上記サービス用サーバからサービス提供が必要とされる特定の電子機器に対して、機器ＩＤを利用して通信網を介してアクセスし、アクセスした電子機器に対して、特定のサービスを実現するための所定内容を有するサービス情報を送信するための送信手段を備えることとした。

また、少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器ＩＤが割り与えられる電子機器と、所定のサービス提供機能を有すると共に、サービス提供可能な複数の上記電子機器についての上記機器ＩＤが格納されるサービス用サーバと、通信網とを備えて成るサービス提供システムとして、電子機器からサービス用サーバに対して通信網を介してアクセスし、特定のサービスに利用可能な所定内容の情報を送信することのできる第１の通信手段と、サービス用サーバからサービス提供が必要とされる特定の電子機器に対して、機器ＩＤを利用して通信網を介してアクセスし、アクセスした電子機器に対して、特定のサービス提供を実現するための所定内容を有するサービス情報を送信するための第２の通信手段とを備えることとした。

また、少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器ＩＤが割り与えられる電子機器と、固有となる端末ＩＤが割り与えられる移動無線端末装置と、通信網とを備えて成るサービス提供システムとして、移動無線端末装

網に接続される認証サーバとから成るものとされる。

そして、通信端末装置が、電子機器に固有となるように割り与えられる機器ＩＤを利用して通信網を介して電子機器にアクセスするのに、認証サーバを経由してのみ上記電子機器にアクセスすることを可能とするアクセス手段と、通信網内において、通信端末装置が通信網に対してアクセスしてきたアクセス経路を特定する情報を利用して、通信端末装置の端末ＩＤを生成する端末ＩＤ生成手段と、認証サーバにおいて、端末ＩＤを利用して、アクセスしてきた通信端末装置についての認証処理を行うとともに、認証が成立した場合にのみ、通信端末装置が電子機器に対してアクセスすることを許可する認証対応処理手段と、認証対応処理手段によってアクセスが許可された通信端末装置と電子機器との間において、通信網を介して特定のサービス提供を実現するための所定内容を有するサービス情報の送受信が行われるようにする送受信手段とを備えることとした。

上記構成においては、例えば家庭内や企業などでほぼ固定的に設置されることで、通信網までのアクセス経路も固定されるような通信端末装置と、移動体に搭載されたり、携帯されることで移動することが想定される電子機器と通信を行うのにあたっては、通信端末装置が、相手側の電子機器の機器ＩＤを利用してアクセスするようにされる。そして、アクセス後におけるサービス情報の送受信によって特定のサービス提供が実現されることになる。

つまりは、この構成によっても、本来は通信網上において不特定多数の端末装置の１つである電子機器に対して積極的にアクセスして通信を行うことでサービスを提供することが可能とされるものである。

そのうえで、上記構成においては、通信端末装置から電子機器へのアクセスにあたって認証サーバが介在することになる。そし

示すブロック図である。

図７は、システムバージョンアップのサービス提供を実現するための処理動作を示すフローチャートである。

図８は、自動車のセキュリティチェックを携帯電話から行うというサービス提供を実現するための処理動作を示すフローチャートである。

図９は、自動車の鍵を、携帯電話からのコントロールにより行うというサービス提供を実現するための処理動作を示すフローチャートである。

図１０は、地図情報の更新データをナビゲーションシステムがサービスサーバからダウンロードするというサービスを実現するための処理動作を示すフローチャートである。

図１１は、本発明の実施の形態としてのサービス提供システム（第２例）の構成例を示す説明図である。

図１２は、パーソナルコンピュータの内部構成例を示すブロック図である。

図１３は、本実施の形態における認証サーバの内部構成例を示すブロック図である。

図１４は、本実施の形態におけるＰＣ－ＩＤ登録手順（第１例）を示す概念図である。

図１５は、本実施の形態におけるＰＣ－ＩＤ登録手順（第２例）を示す概念図である。

図１６は、本実施の形態におけるＰＣ－ＩＤ登録手順（第３例）を示す概念図である。

図１７は、パーソナルコンピュータがナビゲーションシステムの現在位置情報を取得するというサービスを実現するための処理動作を示すフローチャートである。

図１は、本実施の形態の第１例としてのサービス提供システムの一形態例を示している。

自動車１００には、ナビゲーションシステム１が搭載されている。このナビゲーションシステムは、いわゆるカーナビゲーション装置を基本として、自動車の盗難などを防ぐセキュリティティシステム、また、無線電話通信網３００を介してデータ通信が可能な通信端末装置などを備えたシステム構成を採っている。

本実施の形態のサービス提供システムによるサービスを受けるのは、この自動車１００の所有者であり、また、ナビゲーションシステム１を購入したユーザとなる。

携帯電話２００は、例えばナビゲーションシステムと同じユーザの名義で、無線電話通信網３００を運営する通信会社と契約してあるもので、上記のようにして、無線電話通信網３００を介して、電話回線を使用しての通話を行うことができる。また、この場合には、インターネットとの接続によりデータ通信を行うことも可能とされている。

無線電話通信網３００は、例えば携帯電話のほか、本実施の形態であればカーナビゲーション装置の無線端末装置などの、無線端末装置間の移動体通信を実現するための設備とされ、例えば図示するように、基地局３０１、中継局３０２、アプリケーションサーバ３０３，ゲートウエイ３０４を備える。

基地局３０１及び中継局３０２によっては、例えば無線端末装置間での無線通信が可能とされる。また、無線端末装置をインターネットと接続する際には、アプリケーションサーバ３０３がその機能を果たすようにされる。

アプリケーションサーバ３０３は、例えばその無線通信会社で提供するインターネット機能に対応して必要となる処理を実行するようにされている。そして、アプリケーションサーバ３０３に

を示している。

この図２に示す本実施の形態のナビゲーションシステム１は、例えばナビゲーション本体部２、ディスプレイモニタ部３、ＧＰＳアンテナ５、交通情報受信アンテナ７、自律航法ユニット６、通信端末装置５０、セキュリティシステム部４１、及びリモートコントローラ８等によって構成される。

ナビゲーション本体部２の詳しい構成については後述するが、その内部で再生される記録媒体９から読み出した地図情報と、現在位置情報とに基づいて、例えばディスプレイモニタ部３の表示画面３ａに対して、自車の現在位置を地図上に表示させたり、また、ドライブ経路や各種ガイドとなるナビゲーション情報を表示させることができるようになっている。

記録媒体９は、例えばこの場合には、ＣＤ－ＲＯＭ（Compact Disk－Read Only Memory）や、ＤＶＤ－ＲＯＭ（Digital Video Disk／Digital Versatile Disk－Read Only Memory）等のディスクとされ、上記もしたように地図情報が記憶されている。

ディスプレイモニタ部３の表示画面部３ａには、例えば液晶ディスプレイ等によって構成され、ナビゲーション本体部２から出力される画像情報に基づいて表示が行われる。

受信部３ｂはリモートコントローラ８から送られてくるコマンド情報を受信する受信部とされる。この受信情報は、後述するようにして、ナビゲーション本体部２に対して伝送される。

また、ここでは図示していないが、本実施の形態のナビゲーション装置としては、スピーカ等の音声出力部を設けることも可能とされる。その場合は、ナビゲーション本体部２から音声出力部に対して、所定のポイント（交差点）や、渋滞状況、右折左折地点、道順間違い、などといった音声ナビゲーション情報を出力することで、音声出力部からユーザに対して警告音やガイド音声を

、コマンド信号を赤外線輝度変調信号として出力する出力部等を備えており、その赤外線によるコマンド出力が上記受信部３ｂで受信される。

ここで、リモートコントローラ８に備えられる緊急キー８ａは、例えば交通事故や、第三者とのトラブルなどの、搭乗者にとって危険とされる状況が発生したときに操作されるもので、これによって、例えば、そのときの状況を記録した画像、音声データを転送させることができるようになっている。

なお、操作手段としては、これ以外にも、例えば電波送信によるリモートコントローラ、ナビゲーション本体部２と有線接続されるリモートコントローラ、さらにはナビゲーション本体部２やディスプレイモニタ部３の筐体上に設けられる操作部等とされてもよいものである。

通信端末装置５０は、先に図１に示した無線電話通信網３００を介するようにしてインターネットに接続するための移動体通信端末である。そして、この通信端末装置５０は、図示するようにナビゲーション本体部２と接続されることで、ナビゲーション本体部２からデータを無線によって送信することが可能となり、また、通信端末装置５０にて受信したデータを入力して、ナビゲーション本体部２にて所要の処理を実行することが可能となるものである。つまり、通信端末装置５０とナビゲーション本体部２とが接続されることで、本実施の形態のナビゲーションシステム１には、少なくともインターネット接続機能が与えられる。

セキュリティシステム部４１は、自動車自体及び搭乗者を保安するための機能を有するものとされ、この場合には、外付けカメラ４２、マイクロフォン４３、ロックコントロール部４４、及び記憶部４５を備えてなる。

外付けカメラ４２は、例えば実際には、複数のカメラ装置から

タとして記憶部４５への記録が行われる。

ロックコントロール部４４は、自動車の鍵の開閉動作をコントロール可能なように自動車への取り付けが行われる。また、鍵の開閉をコントロール機構部位の状態に応じて、現在、鍵がかかっているか否かを示すロック状態情報をナビゲーション本体部２に対して出力することも可能になっている。

記憶部４５は、例えば比較的大容量のデータを記憶可能な記憶デバイスを備えて成る。ここでは、この記憶部４５として採用されるメディアは特に限定はしないが、例えばハードディスクであってもよいし、また、他のディスクメディアや不揮発性のメモリ素子などが採用されて構わない。本実施の形態の場合には、記憶部４５には、上記した各カメラ装置に撮像された動画像データ、及び、マイクロフォン４３により収音された音声信号データが、自動車内部及び周囲の状況を再現する証拠的な情報として記憶される。

１－３．ナビゲーション本体部の内部構成

図３のブロック図は、ナビゲーション本体部２の内部構成を示している。

この図４において、測位部４は自車の現在位置を測位する部位であり、インターフェイス１４から転送されてくるＧＰＳの受信データや、自車の走行情報に基づいて例えば所定の演算処理を実行することで、自車の現在位置を示す位置情報としての緯度／経度情報を得るようにされる。

ＲＯＭ（Read Only Memory）１１には、本実施の形態のナビゲーションシステム１が所要の処理を実行するための各種プログラム、及び原則として書き換え不可の各種ファクトリープリセット

ション本体部２とを接続するために設けられる。

この場合のインターフェイス１４には、ＧＰＳアンテナ５からの受信データが入力される。また、交通情報アンテナ７にて受信された道路交通情報のデータが入力される。自律航法ユニット６の車速センサにて検出される車速パルスが入力される。また端子３２を介しては、ジャイロ６ｂにて検出される自車の走行方向情報が入力される。

ＧＰＳアンテナ５からの受信データと、自律航法ユニット６からの走行情報（車速パルス及び走行方向情報）は、バス２０を介して測位部４に転送される。測位部４では、これらの転送された情報をパラメータとして入力して、自車の現在位置を測定する。

また、交通情報アンテナ７からの道路交通情報のデータは、例えば制御部１９の制御によってＤＲＡＭ１３に書き込まれて保持されると共に、制御部１９がこのＤＲＡＭ１３に書き込んだ道路交通情報を参照することで、例えばディスプレイモニタ部３に対して表示出力すべき地図情報画像データにおいて渋滞状況等の道路交通情報が反映されるようにも画像処理制御等を実行するようにされる。

時計部１５は、現在日時を計時するもので、その時間情報は、当該ナビゲーションシステム１において必要とされる時間管理のために用いられる。

入力部１６は、ディスプレイモニタ部３の受信部３ｂと接続されており、受信部３ｂで受信したリモートコントローラ８からのコマンド信号が入力される。そして、入力されたコマンド信号を内部バス２０により伝送可能なフォーマットに変換した後、バス２０を介して制御部１９に転送する。制御部１９では、入力したコマンド信号に基づいて適宜所要の制御処理を実行するようにされる。

が行われる。

また、記憶部４５に対して動画像データ及び音声データを記録するのにあたっては、例えば記録を行っていく過程で、記録可能容量が一杯になったときには、最も過去に記録された動画像データ及び音声データを上書き消去していくようにして、最新の撮像画像データ及び音声データを記録していくようにされる。このようにすれば、記憶部４５の記憶容量としては比較的少なくても済む。この記録可能容量としては時間的に例えば数１０分程度であれば、証拠を残すという目的には充分に適うものとされる。

なお、上記画像音声処理部４６としては、例えば、記憶部４５に記録された画像音声データを再生出力するためのデコード機能を備えるようにしても構わない。このようなデコード機能を与えれば、例えば記憶部４５に記録された画像音声データを表示部３にて再生出力させるようにすることも可能とされる。

通信インターフェイス４７は、通信端末装置５０とナビゲーション本体部２との間でのデータの送受信を司る。例えば通信端末装置５０からナビゲーション本体部２側にデータ出力が行われた場合には、通信インターフェイス４７は、通信端末装置５０から入力されたデータを、ナビゲーション本体部２内で処理可能な形式に変換して、データバス２０を介して所要の機能回路部に出力する。

また逆に、ナビゲーション本体部２から通信端末装置５０に対してデータを転送する場合には、通信端末装置５０により処理可能な形式のデータに変換して通信端末装置５０に対して出力するようにされる。

またここでは、通信端末装置５０に対する動作制御は、ナビゲーション本体部２の制御部１９が実行するようにされる。つまり、通信端末装置５０とナビゲーション本体部２とが連携して無線

て入力される。信号処理回路２０４では、この音声信号について所定のエンコード処理を施して送信回路２０３に対して出力する。送信回路２０３では、信号処理回路２０４から入力された信号をアンテナ１を介して送信出力させる。

システムコントローラ２０８は、当該携帯電話による各種動作が行われるように各種制御処理を実行する。

このシステムコントローラ２０８には、ＲＯＭ２１７及びＲＡＭ２１８が備えられる。ＲＯＭ２１７は、例えばフラッシュメモリやＥＥＰＲＯＭなどにより構成される書き換え可能なメモリとされ、ここにシステムコントローラ２０８が実行すべきプログラムや表示データが記憶される。また、例えば電話帳データや、送受信したメールのデータなど、ユーザが設定、登録した各種データも記憶保持される。

更に本実施の形態においては、ＲＯＭ２１７には、この携帯電話２００に対して固有に与えられた携帯ＩＤが付される。これは、携帯電話の場合であれば、割与えられた電話番号の情報としてもよいものである。

キー操作部２１０は、所定複数のボタンキーから成るものとされ、これらボタンキーに対する操作に応じた操作情報信号をシステムコントローラ２０８に対して出力する。システムコントローラ２０８は、この操作情報信号に基づいて、所要の動作が得られるように制御処理を実行する。

また、ＬＣＤ表示部２０９は、図示するように、システムコントローラ２０８の制御によって、動作状況に応じた内容の表示が行われるように駆動される。

なお、ナビゲーションシステム１に備えられる通信端末装置５０の内部構成も、上記図４に示す構成に準じたものとされる。但し、通信端末装置５０の場合には、これをユーザが携帯して通話

、ユーザが所有するナビゲーションシステム１に割与えられたものと同一のナビＩＤのデータが格納される。なお、このナビＩＤとしては、例えば無線端末装置５０に対して割り与えた電話番号とすることが考えられ、ナビＩＤを電話番号とすれば、例えばアプリケーションサーバ３０３、またはサービスサーバ５００から、ナビゲーションシステム１の無線端末装置にアクセスすることを容易に実現できる。

また、例えば携帯電話２００から、無線電話通信網３００を介するようにしてナビゲーションシステム１に対してアクセスする場合には、アクセスを要求した携帯電話２００が適正であることの認証を得るために、携帯電話２００に対してユーザがパスワードの入力操作を行うのであるが、ユーザデータベース４１０のパスワードとしては、この値が格納されることになる。

ところで、図５に示されるユーザデータベース４１０の内容として、各ユーザ個人ごとの情報は、例えば次のような機会において、所要の情報を取得して作成することができる。

例えばナビゲーションシステム１は、インターネットを利用したいわゆるインターネットショッピングにより購入することができるものとしている。このようなインターネットショッピングにより購入手続きを行うのにあたっては、例えばユーザは、ブラウザ画面上に表示される入力フォームに対して所要の個人情報を入力する。また、本実施の形態のようにして無線端末装置５０を備えるナビゲーションシステム１であれば、このナビゲーションシステム１の購入に際して、無線端末装置５０を利用可能とするための通信会社との契約も行うようにされる。本実施の形態では、アプリケーションサーバ３０３（またはサービスサーバ５００）が、インターネットショッピングのための販社サーバと通信することで、これらの情報を受け取り、そしてデータベースとして作

アクセス要求に応じてのインターネットとの接続処理や、ユーザデータベース４１０を検索するためのアプリケーションプログラムなどである。

インターフェイス４０２は、中継局３０２側との情報送受信のために設けられ、インターフェイス４０３は、ゲートウェイ３０４（インターネット）側との情報送受信のために設けられる。

制御部４０４は、実行アプリケーション４１１としてのプログラム内容に従って各種の制御処理を実行する。

１－６．サービスサーバの内部構成

図６は、サービスサーバ５００の内部構成例を簡略に示している。

この図に示すサービスサーバ５００は、記憶部５０１、ネットワークインターフェイス５０２、制御部５０３を備える。

この場合にも記憶部５０１には、各種サービスを提供するサーバとしての機能を実現するのに必要とされる各種情報が記憶されている。ここでは、記憶部５０１に格納される代表的なデータとして、ユーザデータベース５１０、実行アプリケーション５１１、サービス用データ５１２が示される。

ユーザデータベース５１０は、例えば先に図５において説明したユーザデータベース４１０と同様の内容でよいものとされ、例えば、アプリケーションサーバ３０３と通信を行うことで、常に同じ内容を保有しているようにされる。つまり、アプリケーションサーバ３０３またはサービスサーバ５００との何れか一方のサーバにおいて、ユーザの新規契約などによってユーザデータベースの内容が更新されると、他方のサーバに対してユーザデータベースが更新されたことを通知して、互いのユーザデータベースの

ナビＩＤと共に、サービス用データ５１２として最新版のメディアを勧めるコンテンツデータを、無線電話通信網３００のアプリケーションサーバ３０３に対して送信する。このコンテンツデータは、例えば「地図ディスクの新盤がでています。もしよろしければお買い求め下さい。入手方法は・・・・」などのような文字を、表示部３の表示画面３ａに表示出力可能なデータとされる。

アプリケーションサーバ３０３では、ユーザＩＤとコンテンツデータを受信すると、受信したユーザＩＤのナビゲーションシステム１のすべてに対してコンテンツデータを送信する。

そして、このコンテンツデータは、ナビゲーションシステム１の無線端末装置５０にて受信されてナビゲーション本体部２に対して転送される。そして、制御部１９の制御によって、受信したコンテンツデータを、表示部３の表示画面３ａに表示出力させる。このようにして表示されたメッセージの内容を見ることで、ユーザは、新しい地図情報のディスクがメーカ側から提供されていることを知ることができる。

なお、このようなコンテンツデータを受信したときに、ユーザが必ず自動車に搭乗していて表示画面３ａに表示されるコンテンツデータを見ることができるとは限らない。そこで、例えば運転が行われていないなどして、ナビゲーションシステム１のメイン電源が入っていないようなときには、無線端末装置５０によりコンテンツデータを受信したときに、自動的にメイン電源をオンとして、受信して取得したコンテンツデータをメモリ１２や記憶部４５に記憶させておくようにされる。そして、例えばユーザが自動車のイグニッションキーを回して、ナビゲーションシステム１のメイン電源がオンとなったときに、このコンテンツデータを表示画面３ａに表示させるようにすることも考えられる。

もしくは、ナビゲーションシステム１が動作している状態のも

バージョンアップが行われることになる。しかも、この場合にはバージョンアップが自動的に行われるため、ユーザにとっては非常に有用なサービスとなるものである。

また、携帯電話２００をユーザが利用して操作を行うことで、遠隔地から自動車についてのセキュリティに関するコントロールを行えるようにすることも可能とされる。この動作についても簡単に説明する。

例えば、ユーザは、携帯電話２００を操作して、無線電話通信網３００のアプリケーションサーバ３０３に対してアクセスする。ここでアクセスするのは、自動車のセキュリティコントロールのためのサーバ（アプリケーションサーバ３０３に在るものとする）とされる。そして、更にユーザは所定操作を行うことで、自動車の鍵がロックされているか否かについての問い合わせを行う。このリクエストに応じて、アプリケーションサーバ３０３内のセキュリティサーバは、アクセスしてきた携帯電話と同じユーザが所有するナビゲーションシステム１のナビＩＤを検索して、この検索されたナビＩＤのナビゲーションシステム１に対して、キーロック問い合わせのコマンドを送信する。

このコマンドを受信したナビゲーションシステム１では、セキュリティシステム部４１のロックコントロール部４４からの情報に基づいて、現在鍵がロックされているか否かについてのキーロック情報を、アプリケーションサーバ３０３に送信する。アプリケーションサーバ３０３は、このキーロック情報を、携帯電話２００に対して転送するようにして送信する。携帯電話２００では、例えばキーロック情報に基づいて、ユーザの自動車の鍵がかかっているか否かの情報を、例えば表示などによって示すようにされる。

そして、例えば鍵がかかっていないとすると、ユーザは、携帯

限定はしないが、ここでは、例えば更新前の地図情報との差分データのみを有しているものとする。つまり、例えば新たな道路を地図上に加えるようにして更新が行われているとすれば、この新たな道路をしかるべき位置に表示させるための差分データが更新データとされることになる。このようにして、更新データを差分データの形式とすれば、例えばサービスサーバ５００では、サービス用データ５１２に格納すべき更新データとして、更新内容を含む全地図情報を記憶する必要はなくなるので、それだけ、記憶部８０１の記憶容量を節約することができる。

この場合の地図情報が更新されたことのユーザへの通知は、先の地図情報を記録したメディアの最新版の購入を勧めるコンテンツデータの送信と同様にして行えばよいものとされる。そして、送信されたコンテンツデータがナビゲーションシステム１にて表示されることで、例えばユーザは、地図情報が更新されており、また、この更新データをダウンロードして取得可能であることを知ることができる。

そして、ユーザが地図情報の更新データを取得したいと思った場合には、例えば、地図情報のダウンロードを指示するための所定操作をナビゲーションシステム１に対して行うようにされる。この操作は、例えば上記したコンテンツデータとして含まれているＸＭＬやＨＴＭＬなどによるダウンロード用のアプリケーションをＧＵＩとして表示画面3 aに表示させ、このＧＵＩに対して所定操作を行うことができるように構成することが考えられる。

上記のようにして操作が行われたとすると、ナビゲーションシステム１においては、例えば制御部１９の制御によって、自身のナビＩＤと共に、更新データのリクエストを送信することになる。この送信データは、通信端末装置５０から無線電話通信網３００に対して送信され、無線電話通信網３００内のアプリケーショ

データが受信されることになる。

そして、ナビゲーションシステム１側においては、受信した更新データを記憶しておくようにされる。以降においては、この更新データを利用することで、地図上の現在位置表示や各種ガイド情報の表示などのナビゲーション動作として、更新データの内容を反映させることが可能となるものである。

また、ユーザにとってメリットのあるサービスではないが、ナビゲーションシステム１の購入後におけるユーザに対する対応として、次のようなことを行うこともできる。

この場合、サービスサーバ５００としては、ユーザが分割払いによってナビゲーションシステム１を購入した際には、その支払い状況のデータベースが格納されているものとされる。そして、上記したデータベースの内容から、ユーザの支払いが或る限度以上にまで滞っていることが分かった場合には、サービスサーバ５００側から、例えば「代金支払いを御願いします。代金支払いの確認がとれるまで、ナビの利用を停止いたします。」というメッセージと、制御情報を送信する。これを受信したナビゲーションシステム１では、表示画面３ａに上記した内容のメッセージを表示させると共に、以降においては、ナビゲーションシステム１自体がその動作を停止させてしまうようにするものである。

また、本実施の形態のナビゲーションシステム１は、先にも述べたように、単体でも購入可能であるが、自動車保険の購入時においてこれと組み合わせて購入することも可能とされ、例えばこのようにして組み合わせて購入した場合には、両者の金額が更に割り引かれたり、また、分割払いの金利手数料が割り引かれるなどのサービスが行われる。そして、このようにして組み合わせによる購入を行った場合に、上述のようにして代金支払いが滞っている場合には、ナビゲーションシステム１の利用の停止と共に、

る。つまり、本実施の形態としては、サーバ側からのアクセスにより、例えば適切とされる機会に、適切な内容のサービスをナビゲーションシステム１に対して積極的に提供することができるものである。

３．処理動作例

続いては、上記のようにして例示した各種サービスのうちから選択したいくつかのサービスを実現する際の処理動作について説明していくこととする。

先ずは、サービスサーバ５００が提供する、ナビゲーションシステム１のバージョンアップのサービスを実現するための処理動作について、図７のフローチャートを参照して説明する。なお、この図においては、サービスサーバ５００、アプリケーションサーバ３０３、及びナビゲーションシステム１の各々において実行される処理が並列的に示される。また、サービスサーバ５００としての処理は制御部５０３が実行し、アプリケーションサーバ３０３としての処理は、制御部４０４が実行し、ナビゲーションシステム１としての処理は制御部１９が実行する。

例えば、メーカ側によりサービスサーバ５００に対してナビゲーションシステム１のシステムのバージョンアップをすべきであるとの指示が行われたとすると、サービスサーバ５００の制御部５０３は、ステップＳ１０１としての処理により、或る特定のナビゲーションシステム１に対するアクセス要求を行う。この際には、アクセス要求と共に、アクセスすべきナビゲーションシステム１のナビＩＤを送信する。このナビＩＤは、例えば、バージョンアップが必要とされるナビゲーションシステム１の機器を所有しているユーザをユーザデータベース５０１のユーザ情報から検

受信したレスポンスに格納されるバージョンナンバ及びナビＩＤを抽出して、これらの情報を、サービスサーバ５００に対して送信する。

サービスサーバ５００は、ステップＳ１０３によりアプリケーションサーバ３０３からのバージョンナンバの通知を受けると、ステップＳ１０３において、この通知されたバージョンナンバに基づいて、バージョンアップが必要であるか否かについて判別する。例えば通知されたバージョンナンバが今回のアップデータのバージョンナンバ以上であれば、バージョンアップは不要とされて否定結果が得られるが、今回のアップデータのバージョンナンバよりも小さければバージョンアップが必要であるとして肯定結果が得られることになる。

ここで否定結果が得られれば、このナビＩＤを有するナビゲーションシステム１に対する通信（アクセス）はこれ以上実行しないようにされるが、肯定結果が得られたのであれば、次のステップＳ１０４の処理によって、バージョンアップメッセージと、アップデータをナビＩＤと共にアプリケーションサーバ３０３に対して送信する。これらバージョンアップメッセージとアップデータは、サービスサーバ５００の記憶部５０１においてサービス用データ５１２として格納してあるものを読み出すことで得るようにされる。

アプリケーションサーバ３０３においては、ステップＳ２０５において、バージョンアップメッセージ、アップデータ、ナビＩＤを受信する。そして、続くステップＳ２０６により、受信したナビＩＤのナビゲーションシステム１に対して、バージョンアップメッセージと、アップデータを送信する。

ナビゲーションシステム１においては、バージョンアップメッセージとアップデータを無線端末装置５０にて受信して、ナビゲ

先ず、図８には、自動車の鍵をかけたかどうかについての問い合わせを携帯電話２００から自動車に対して行うための処理動作が示される。

例えばユーザが携帯電話２００に対する所定操作を行うことによって、ステップＳ４０１として示す、セキュリティリクエストを端末ＩＤと共に送信するための処理が実行される。このためには、例えば先ず、携帯電話２００が通信を行ってアプリケーションサーバ３０３内で運営されているとされるセキュリティシステムのサーバにアクセスするようにされる。そして、このサーバに対して、自分が所有する自動車についてのセキュリティの問い合わせを要求するものである。この際、自分以外のユーザによる悪用を防止するために、ユーザが予め登録してあるパスワードの入力が求められる。

上記したセキュリティリクエスト、端末ＩＤ、及びパスワードをステップＳ５０１により受信したアプリケーションサーバ３０３（セキュリティシステムのサーバ）では、ステップＳ５０２の処理として、先ずユーザデータベース４１０を参照して、パスワードと端末ＩＤなどとの照合を行うことで認証処理を実行する。つまり、セキュリティリクエスト、端末ＩＤ、及びパスワードを送信したユーザが正規のユーザであることについての確認を行う。なお、この時点で認証が得られなければ、以降の処理は停止される。

そして適正に認証が得られたとされると、次のステップＳ５０３において、そのユーザデータベース４１０において、認証された端末ＩＤ及びパスワードに対応付けられたナビＩＤを検索して得る。そして、続くステップＳ５０４により、取得したナビＩＤ（電話番号）を有するナビゲーションシステム１に対してセキュリティリクエストを送信する。

携帯電話２００では、この送信されたセキュリティチェックの結果データが着信したことをステップＳ４０２にて判別すると、これを受信して、次のステップＳ４０３において、例えばＲＯＭ２１７に対して記憶させるようにしている。そして、例えばこの後において、ユーザが所定操作を行うことで、ステップＳ４０４としての処理によって、このセキュリティチェックの結果を文字等によりＬＣＤ表示部２０９に表示させることができるようになっている。

そして、例えばＬＣＤ表示部２０９に表示させたセキュリティチェックの結果から、自動車に鍵がかかっていないことをユーザが知った場合には、前述したようにして、携帯電話２００からのリモートコントロールによって、自動車の鍵をかけることが可能とされている。このための処理が図９に示される。

ここでは、例えばユーザの所定操作に応じて、ステップＳ７０１の処理によって、携帯電話２００のインターネット接続機能を利用してアプリケーションサーバ３０３に対してアクセスする。そして、自動車の鍵をかけることを指示するためのキーロック指示情報を、携帯ＩＤとパスワードと共に送信する。

アプリケーションサーバ３０３では、ステップＳ８０１としての処理によって、上記キーロック指示情報、携帯ＩＤ、及びパスワードを受信すると、先ず、ステップＳ８０２の処理によって認証処理を実行する。この認証処理は、図８のステップＳ５０２における認証処理と同様となる。そして、適正な認証結果が得られたのであれば、ステップＳ８０３に進む。

ステップＳ８０３においては、ユーザデータベース４１０を参照することで、携帯ＩＤと対応付けられたナビＩＤを検索する。そして、次のステップＳ８０４において、検索したナビＩＤを有するナビゲーションシステム１に対してキーロックコマンドを送

をステップＳ２１により受信したアプリケーションサーバ３０３では、次のステップＳ２２の処理として、ユーザデータベース４１０を参照して、登録されているパスワードとナビＩＤなどとの照合を行うことで認証処理を実行する。つまり、更新データのリクエストを送信したユーザが正規のユーザであるか否かについての確認を行う。なお、この場合にも、認証が得られなければ以降の処理は停止される。

そして適正に認証が得られたとされると、次のステップＳ２３において、先のステップＳ２１にて受信したとされるリクエストとナビＩＤを、サービスサーバ５００に対して送信する。

サービスサーバ５００では、ステップＳ３１の処理として、アプリケーションサーバ３０３から送信されたリクエストとナビＩＤを受信すると、次のステップＳ３２において、記憶部５０１にてサービス用データ５１２として記憶されている、地図情報の更新データのファイルについての読み出しを行う。

なお、この更新データは、例えば前述もしたように、更新前の地図情報としてのデータに対する差分データとされればよい。また、ここでは、全ての更新データファイルについて読み出しを行ってもよいが、例えば、この更新データが商品として購入されるものであって、例えばユーザが指定した地域数等に応じてその価格が代わるように設定することも考えられる。そこで、このような場合であれば、リクエストとしては、ダウンロードすべき更新データファイルを指定する情報を含むようにして、この指定された更新データファイルのみについての読み出しを行うようにしてもよい。

上記のようにして更新データファイルの読み出しが行われると、続いては、ステップＳ３３の処理によって、読み出した更新データファイルを、先にステップＳ３１においてリクエストと共に

映されたナビゲーション動作が得られることになる。

また、記録媒体９が書き換え不可である場合には、例えば電源がオフとなっても記憶内容が維持されるメモリ１２若しくは記憶部４５などに受信した更新データを記憶させておく。そして、地図情報を利用した表示を行うような場合には、例えばメモリ１２若しくは記憶部４５に記憶されている更新データを読み出して、記録媒体９から読み出した地図情報に合成させて、更新データが反映された地図情報を形成する。そして、この地図情報を利用してナビゲーション動作を行うようにされる。

なお、先にも述べたように、このような更新データの提供サービスは、有料とすることも無料とすることも考えられるが、有料であるとすれば、ナビゲーションシステム１から送信されたダウンロードのリクエストをサーバ側で受信したときに、例えばユーザが指定した支払方法に応じた決済の処理が行われるようにすればよい。

４．サービス提供システム（第２例）

４－１．全体構成

続いては、実施の形態の第２例としてのサービス提供システムについて説明していくこととする。

図１１は、第２例としてのサービス提供システムの一形態例を示している。

この図に示されるように、第２例としては、図１に示した第１例のシステム構成に対して、装置としては、パーソナルコンピュータ７００と、認証サーバ８００が追加された構成を採っている。そこで、図１１の説明にあたっては、これらの追加部分等の相

例えばほかには、ＩＳＤＮ(Integrated Services Digital Network)、また、電話回線の高周波帯域を通信に利用したＡＤＳＬ(Asymmetric Digital Subscriber Line)等をはじめとするｘＤＳＬ、ＣＡＴＶ、無線通信網などを挙げることができる。

認証サーバ８００は、例えば後述するようにして、パーソナルコンピュータ７００が自動車１００の現在位置情報を得るために、自動車１００に搭載されているナビゲーションシステム１に対してアクセスする際に、このアクセスが適正なものであるか否かについて認証を行うために設けられている。この認証サーバ８００が機能することによって、結果的には、例えばいわゆる成りすましによって、正規に登録されていないパーソナルコンピュータが自動車１００から現在位置情報を得るという不正行為を防止するようにされる。

なお、認証サーバ８００の内部構成及びその動作については、後述する。

４－２．パーソナルコンピュータの内部構成

図１２は、パーソナルコンピュータ７００の内部構成例を示している。

この図に示すパーソナルコンピュータ７００は、インターネット４００を介しての通信を行うために、ネットワークインターフェイス７０９を備えている。ネットワークインターフェイス７０９は、アクセス用通信網６００と当該パーソナルコンピュータ７００との通信を司るのであるが、これによって、パーソナルコンピュータ７００は、アクセス用通信網６００を介してインターネット４００と接続されることになる。

ＣＰＵ７０１は、例えばハードディスクドライブにインストー

照して説明する。

この図に示す認証サーバ８００は、記憶部８０１、ネットワークインターフェイス８０２、制御部８０３を備える。

認証サーバ８００の場合、記憶部８０１には、後述する認証処理等を実行するのに必要とされる情報が記憶されている。ここでは、記憶部８０１に格納されるデータとして、認証用ユーザデータベース８１０、実行アプリケーション８１１が示される。

認証用ユーザデータベース８１０は、例えば図の下側に示すように、１ユーザごとに、ユーザ情報、携帯ＩＤ、ナビＩＤ、ＰＣ－ＩＤ、コンテンツＩＤ、及びＰＣ用パスワードが対応づけられて格納される。

ユーザ情報は、ナビゲーションシステム１、携帯電話２００、及びパーソナルコンピュータ７００を組として所有するユーザに関する情報であり、例えば本実施の形態のシステムの場合であれば、サービスサーバ５００（又はアプリケーションサーバ３０３）に格納されるユーザデータベース５１０（４１０）を形成するユーザ情報と同じ内容とされればよい。

携帯ＩＤは、ユーザＩＤによって特定されるユーザが所有する携帯電話に書き込まれている携帯ＩＤと同一のデータが格納される。ナビＩＤも同様にして、ユーザが所有するナビゲーションシステム１に割与えられたものと同一のナビＩＤのデータが格納される。また、このナビＩＤとして、無線端末装置５０に対して割り与えた電話番号とされればよい。つまり、この場合の携帯ＩＤ及びナビＩＤは、図５にて説明したユーザデータベース構造において格納される情報と同じ情報が格納されればよいものである。

ＰＣ－ＩＤは、ユーザＩＤによって特定されるユーザが所有するとされるパーソナルコンピュータ７００を識別するためのＩＤとされる。本実施の形態としては、このＰＣ－ＩＤの構造に特徴

るユーザが、現在、自己の所有しているナビゲーションシステム１を搭載している自動車１００の現在位置を知りたいと思ったとする。この場合、ユーザは、パーソナルコンピュータ７００上で、例えばＷｅｂブラウザのアプリケーションを起動させた上で、所定操作を行って、現在位置通知サービスのＷｅｂサイトにアクセスするようにされる。この現在位置通知サービスのＷｅｂサイトは認証サーバ８００にてアップロードしているＷｅｂサイトとされる。つまり、ユーザが現在位置通知サービスのＷｅｂサイトにアクセスしたことによって、パーソナルコンピュータ７００は、認証サーバ８００にアクセスしたこととなる。

上記のようにして認証サーバ８００に対してアクセスしたとすると、ユーザは、現在位置情報通知のためのリクエストを送信するようにされる。また、この現在位置情報通知のリクエストとともに、認証サーバ８００が認証で用いるべき所要の認証情報も送信するようにされる。

なお、認証情報がどのようなものであるのかについては後述する。

また、認証サーバが認証に用いる認証情報としては、リクエストを送信したパーソナルコンピュータ７００に固有となるＰＣ－ＩＤを含むが、このＰＣ－ＩＤは、パーソナルコンピュータ７００にて生成して送信されるのではなく、パーソナルコンピュータ７００が接続されるアクセス用通信網６００内において、例えばアプリケーションサーバとして機能する部位が、パーソナルコンピュータ７００が認証サーバ８００にアクセスしてきたときに生成するようにされる。このＰＣ－ＩＤの生成及びユーザデータベース８１０への登録についても後述することとする。

認証サーバ８００では、上記のようにして、現在位置情報通知のリクエストと共に送信されてきた認証用情報と、ユーザデータ

に、ユーザがパーソナルコンピュータ７００を認証サーバ８００にアクセスさせ、所定の登録のための操作を行うことで登録が行われるようにすることが考えられる。

つまり、ユーザはパーソナルコンピュータ７００を操作して、例えば認証サーバ８００における登録用のＷｅｂページにアクセスする。このＷｅｂページには図１３に示した認証用ユーザデータベース８１０を構築するのに必要とされる、１ユーザについての所要の情報項目を入力することができるようになっている。つまり、「ユーザ情報」となる氏名、住所等をはじめとする個人情報、ユーザが所有する携帯電話２００の「携帯ＩＤ（電話番号）」、同じくユーザが所有するナビゲーションシステム１の「ナビＩＤ（電話番号）」、及び「サービスＩＤ」に対応する享受したいサービス内容（この場合には、現在位置通知サービスとなる）を入力するようにされる。例えば認証サーバ８００においては、現在位置通知サービス以外のサービスも対応して認証を行うような構成とすることも充分に考えられるが、サービスＩＤは、このような場合において、ユーザがサービスの提供を要求してきたときに、そのサービスが何であるのかを識別するのに用いることができる。

また、例えば本実施の形態としての現在位置通知サービスに関すれば、携帯電話２００はこのサービスを享受するのに利用はしていないので、必ずしも、携帯ＩＤを認証用ユーザデータベース８１０の情報要素とする必要はない。しかし、やはり、認証サーバ８００において現在位置通知サービス以外のサービスも対応して認証を行うこととして、その他のサービスが携帯電話２００を利用するものであるような場合には、携帯ＩＤが必要となるものである。

また、図１３によれば、上記「ユーザ情報」「携帯ＩＤ（電話

テム構成に加えたとすると、このパーソナルコンピュータ７００は、無線電話通信網３００にアクセスすることなく、例えば電話回線等をはじめとする何らかのアクセス用通信網６００を介してインターネットにアクセスすることになる。このような場合には、前述した成りすましの問題が生じてくるわけであり、この問題を解決する必要が生じてくるものである。

そこで本実施の形態としては、次のようにしてＰＣ－ＩＤを生成して認証サーバに登録することで、機器ＩＤを改竄しての成りすましによる不正なサービスの享受ができないようにする。なお、ここではアクセス用通信網６００として実際に利用される通信網の種類に応じて、３例を挙げることとする。

図１４は、ＰＣ－ＩＤ登録手順の第１例を模式的に示している。この第１例は、アクセス用通信網６００が一般電話回線、若しくはＩＳＤＮ回線とされている場合である。

アクセス用通信網６００が一般電話回線、若しくはＩＳＤＮ回線などの場合、パーソナルコンピュータ７００がインターネットと接続されるためには、いわゆるダイヤルアップを行うことになる。つまりは、ここでは図示していないが、パーソナルコンピュータ７００側が備えるとされるモデム、ＴＡ(Terminal Adapter)、ＤＳＵ(Digital Service Unit)から、アクセス用通信網６００において一般電話回線又はＩＳＤＮ網として実際に配置される設備である電話局６０１に対してダイヤリングをして接続する。

ここで、留意すべきなのは、上記電話局６０１に対してダイヤルアップを行うということは、このダイヤルアップを行うために割り当てられた電話回線、ＩＳＤＮ回線についての電話番号が一義的に決まっているということである。この電話番号は、電話局６０１にて管理している以上、パーソナルコンピュータ７００のユーザによっては改竄することのできない情報であるといえる。

６０１側にて管理するものであり、かつ、ＰＣ－ＩＤは電話局６０１側にて作成するものであるから、パーソナルコンピュータのユーザが、この電話番号部分を書き換えることは不可能である。従って、パーソナルコンピュータについていわゆる成りすましを行うことは不可能となるわけである。

そして、電話局６０１からは、このようにして生成したＰＣ－ＩＤをインターネットを介して認証サーバ８００に送信することになる。

このＰＣ－ＩＤを受信した認証サーバ８００では、手順③として示すように、受信したＰＣ－ＩＤを、他の情報（ユーザ情報、携帯ＩＤ、ナビＩＤ、及びサービスＩＤ）と共に、認証用ユーザデータベース８１０に登録するようにされる。

また、ＰＣ－ＩＤ登録手順の第２例を図１５に示す。この第２例は、アクセス用通信網６００がＡＤＳＬなどの常時接続が可能な通信網とされている場合である。

このような通信網である場合、例えばアクセス用通信網６００における設備である電話局６０１においては、例えば電話回線を、一般電話回線とインターネットの経路とに分岐するスプリッタなどのポート部が設けられることになるのであるが、この図においては、このようなポート部を接続ポート６０２，６０２・・・として示している。

例えば、電話局６０１では、加入者がＡＤＳＬに加入したときに接続ポート６０２の工事を行って加入者の電話回線と接続するようにしている。従って、この接続ポート６０２については、電話局６０１側が管理するものであると共に、接続される電話回線も固定的なものとなっているといえる。

そこで、本実施の形態としては、例えば電話局６０１において接続ポート６０２ごとに識別子（ポートＩＤ）を割与えて管理す

ソナルコンピュータ７００が常時接続される。

このような場合、パーソナルコンピュータ７００は、専用線６１０において備えられるとされるルータ６１１に対して接続され、このルータ６１１からインターネット４００への接続が行われる。そして、この場合には、パーソナルコンピュータ７００は、ルータ６１１に対して常時接続されているのであるから、パーソナルコンピュータ７００とルータ６１１との経路は固定されていることになる。また、このルータ６１１の管理も専用線６１０側の運営者によって行われていることになり、このルータ６１１に関する情報をパーソナルコンピュータ７００側のユーザが改竄することはできないとされる。

そこで、第３例としては、パーソナルコンピュータ７００の機器ＩＤと、ルータ６１１に固有となる情報を利用してＰＣ－ＩＤを形成するようにされる。そして、この場合には、ルータ６１１に固有となる情報としては、ルータ６１１に割り当てられたルータアドレスを使用することとする。

そして、この第３例としてのＰＣ－ＩＤ登録手順は以下のようになる。

先ず、手順①として、パーソナルコンピュータ７００からは、認証サーバ８００に向けて機器ＩＤを送信する。この場合においても、機器ＩＤの送信は、実際には、「ユーザ情報」「携帯ＩＤ（電話番号）」、「ナビＩＤ（電話番号）」、及び「サービスＩＤ」の各情報とともに送信するものとされる。

但し、この場合の機器ＩＤとしては、先の第１例及び第２例の場合のようにして、メーカコード－製造番号から成る情報を使用してもよいのであるが、常時接続されていることを前提とすると、例えばＤＨＣＰ(Dynamic Host Configuration Protocol)によるものであるとしても、最初にＩＰアドレスの割り当てが行われ

これまでの説明からも理解されるように、アクセス用通信網６００と接続するまでの通信経路は、パーソナルコンピュータ７００が例えば屋内等において固定的に設置されるということを前提にすれば、そのパーソナルコンピュータ７００と通信経路とは１対１で固定的に対応するものとなる。従って、上記通信経路を特定する情報と機器ＩＤとを組み合わせたとしても、パーソナルコンピュータ７００に固有となるＰＣ－ＩＤを形成するのに何ら問題はないことになる。また、先の説明でも述べたようにして、通信経路を特定する各情報（電話番号、接続ポートのポートＩＤ、ルータアドレス）は、何れもアクセス用通信網６００を運営する設備側で管理しているものであり、悪意のパーソナルコンピュータ７００のユーザがこれを改竄することはできないとされる。従って、この情報を利用して生成されるＰＣ－ＩＤをパーソナルコンピュータ７００のユーザが改竄することもできないわけである。また、本実施の形態としては、ＰＣ－ＩＤは、パーソナルコンピュータ側ではなく、中継点であるアクセス用通信網６００の設備側で生成するようにされていることによっても、改竄される可能性を著しく低いものとしている。

つまり、本実施の形態のＰＣ－ＩＤとしては、パーソナルコンピュータを特定可能としながら、かつ、改竄による成りすましを防止することのできる情報となっているものである。これによって、先にも述べたように、成りすましによるパーソナルコンピュータ７００を利用してのサービスの提供が行われるのを防止することが可能となる。

なお、本発明としては、パーソナルコンピュータ７００が最初に接続される通信網（アクセス経路）を特定できる情報でありさえすればよく、上記図１４～図１６により例示した登録手順におけるＰＣ－ＩＤの生成例以外にも、本発明に適合するＰＣ－ＩＤ

際には、ユーザ情報、機器ＩＤ、及びサービスＩＤを共に送信するようにされる。

例えば現在位置通知サービスのブラウザ画面上には、リクエストに必要とされる各種項目を入力する入力ボックスが表示されるようになっているものとされる。上記ユーザ情報は、この入力ボックスに入力した例えば住所、氏名等の個人情報に基づいて、ユーザを特定するＩＤとしてＣＰＵ７０１が作成する。

また、機器ＩＤは、例えばこれがメーカコードと製造番号から成るものであるとすれば、ＣＰＵ７０１が例えばＲＯＭ７０２から読み出したメーカコード、製造番号の情報に基づいて作成することになる。また、機器ＩＤがＩＰアドレスであれば、例えばＲＡＭ７０３に保持しているＩＰアドレスを利用して作成する。

また、サービスＩＤは、例えば、このリクエストが現在位置通知サービスに対応したものであることを示すＩＤとして、現在位置通知リクエストとしてのデータ構造内に格納されているものとする。

上記のようにして送信された現在位置通知リクエストは、図１４～図１６にて説明したようにして、先ずは、アクセス用通信網６００にてルーティングされ、インターネット４００を介して認証サーバ８００に転送されることになる。そして、この際において、アクセス用通信網６００の設備においては、受信取得した機器ＩＤと、自身が管理して保有しているとされる経路特定情報（電話番号、ポートＩＤ、ルータアドレスなど）を利用してＰＣ－ＩＤを作成する。従って、認証サーバ８００に対しては、現在位置通知リクエストと共に、このＰＣ－ＩＤと、ユーザ情報、サービスＩＤが送信されることになる。

認証サーバ８００では、上記のようにして送信されてきた現在位置通知リクエスト、ユーザ情報、ＰＣ－ＩＤ、及びサービスＩ

は、ステップＳ６１の処理によって現在位置通知リクエストを受信することになる。

ここで、本実施の形態のナビゲーションシステム１は現在位置通知サービスに対応したプログラムを格納している。このプログラムは、受信した情報が現在位置通知リクエストである場合には、測位部４にて測定される現在位置情報と、例えば記録媒体９等から読み出した地図情報とを利用して現在位置情報を作成し、認証サーバ８００にアクセスして送信を行うという動作を実行させるものである。なお、現在位置情報の生成に利用する地図情報としては、例えば前述したようにして取得した更新データがあれば、この更新データも利用するようにされる。そして、次に述べるステップＳ６２～Ｓ６４の処理は、このプログラムに従って実行される。

ステップＳ６２においては、現在位置情報を作成する。

前述もしたように、ここで作成される現在位置情報は、例えばＷｅｂブラウザによって表示可能なＨＴＭＬやＸＭＬなどの形式とされ、Ｗｅｂブラウザ上で再生すれば、地図上に現在位置が示される画像を表示させることができるデータ内容を有しているものとされる。なお、例えばＪＰＥＧ、ＪＩＦ、及びビットマップなどをはじめ、単に所定の形式による画像データとして生成することも考えられる。

そして、次のステップＳ６３においては、ナビゲーションシステム１が認証サーバ８００に対してアクセスするための制御処理を実行する。このため、例えばナビゲーションシステム１においては、例えばメモリ１２などに認証サーバ８００のＵＲＬが保持されているものとされ、制御部１９は、このＵＲＬにアクセスが行われるように、通信インターフェイス４７から通信端末装置５０を介してアクセス要求を送信させる。

また、認証サーバ８００としては、例えば当然のことではあるが、１つの装置としてではなく、例えば処理負担の軽減のために、認証サーバ８００として機能する複数の装置が、インターネット上において分散するようにして設けられた構成としても構わないものである。

また、不正行為を防止する構成としては、次のような構成を補助的に付加することも考えられる。

例えば本実施の形態としてのサービス提供システムにおいて、ユーザがサービス提供に利用するものとして登録している各機器（ナビゲーションシステム、携帯電話、パーソナルコンピュータ等）のインターネットの接続を、特定の１つの通信会社（電話会社等）が行うとする。そして、例えばこの通信会社がカバーする範囲の通信網内において監視サーバを設けるようにする。監視サーバは、ユーザが登録している各機器間の通信として、この通信会社がカバーする一定範囲内の回線を利用しているか否かを監視するようにする。そして、通信会社がカバーする一定範囲外の回線から入ってくるようにして、ユーザが登録している機器が通信を行う状況となった場合には、何らかの警告を与えたり、また、不正のサービス利用が行われるような回線の利用状況であるとする場合には、通信を中断させるようにするものである。

また、本発明としては上記した各実施の形態に限定されるものではない。例えば、提供すべきサービスとしては、これまで例示したもの以外にも各種考えられる。また、サービス提供に利用される機器としては、カーナビゲーション装置、携帯電話、パーソナルコンピュータ等に限定されるものではなく、例えばインターネットなどのネットワークとの接続機能を有する移動通信端末装置を備える機器や、また、移動通信端末装置ではなくとも、特定の通信網を介してインターネットと接続される通信端末装置を備

ムを購入したユーザにとっては、サービス提供をこれまでよりも簡易で有効なかたちで享受することができ、また、販売側の両者にとっては製品の付加価値が高まるので、販売促進の効果も期待できることになる。

また、屋内等に固定的に設置される通信端末装置（パーソナルコンピュータ）から電子機器（例えばナビゲーションシステム）に対して通信を行う場合においては、認証サーバを介在させるようにしている。また、通信端末装置が電子機器と通信するために認証サーバにアクセスしたときには、アクセス経路を特定する情報（電話番号、ポート番号、ルータアドレス等）を利用して端末ＩＤ（ＰＣ－ＩＤ）を生成するようにしている。そして、認証サーバでは、端末ＩＤを利用して認証処理を行うようにしている。

アクセス経路を特定する情報は、通常は、通信端末装置が最初に接続する通信網を運営する側が管理保持していることから、通信端末装置側にて改竄することは不可能な情報であり、従って、端末ＩＤとしても改竄することのできない情報であるといえる。つまり、この発明によっては、いわゆる成りすましによって不正なサービス利用が行われることを、簡易な構成によって確実に防止することができるものである。

産業上の利用の可能性

この発明は、例えば自動車などの移動体に搭載される電子機器と、サーバ及び携帯電話などの個人移動端末装置とを通信網を介して通信可能なように構築されたシステムとして、例えば電子機器を購入して利用しているユーザに対して、送信されたデータを受信した電子機器が、その受信データの内容に従って何らかの動作の実行を行うことで享受できるようなサービスを提供することのできるシステムに利用される。

有となる端末ＩＤが割り与えられる移動無線端末装置と、通信網とを備えて成り、

上記移動無線端末装置から上記電子機器に対して、上記機器ＩＤを利用して上記通信網を介してアクセスし、特定のサービス提供を実現するための所定内容を有するサービス情報を送信するための送信手段、

を備えていることを特徴とするサービス提供システム。

4．少なくとも、無線通信端末機能を備えて移動体に搭載されると共に、固有となる機器ＩＤが割り与えられる電子機器と、固有となる端末ＩＤが割り与えられる移動無線端末装置と、通信網とを備えて成り、

上記電子機器から上記移動無線端末装置に対して、上記端末ＩＤを利用して上記通信網を介してアクセスし、特定のサービスに利用可能な所定内容の情報を送信することのできる第１の通信手段と、

上記移動無線端末装置から特定の電子機器に対して、上記機器ＩＤを利用して上記通信網を介してアクセスし、アクセスした電子機器に対して、特定のサービス提供を実現するための所定内容を有するサービス情報を送信するための第２の通信手段と、

を備えていることを特徴とするサービス提供システム。

5．少なくとも、無線通信端末機能を備えて移動体に搭載される電子機器又は移動無線端末装置としての電子機器と、通信網と、該通信網にアクセスする経路が固定的となるようにして設置される通信端末装置と、上記通信網に接続される認証サーバとから成り、

上記通信端末装置が、上記電子機器に固有となるように割り与えられる機器ＩＤを利用して上記通信網を介して上記電子機

報とに基づいて判断して上記無線通信装置を制御する認証装置とを備える通信システム。

7．上記通信システムは、

通信機能を備えるとともに機器毎に異なる第2の機器ＩＤを備える第2の電子装置と、

上記第2の電子装置と通信を行うと共に上記ネットワークに接続され、上記第2の機器ＩＤを上記第2の電子装置から受信し、上記第2の電子装置と通信を行う通信手段を特定する通信手段ＩＤと上記第2の機器ＩＤとを上記認証装置に送信する通信装置

を更に備える第6記載の通信システム。

8．上記認証装置の備えるグループ情報は、上記第2の電子装置を上記第2の機器ＩＤと上記通信手段ＩＤとを関連づけて更に管理する第7項記載の通信システム。

9．ネットワークに接続され各々の機器を識別可能とするための機器ＩＤを各々備えるとともに送信可能な複数の他の電子機器の間の通信を制御する通信装置において、

上記ネットワークを通して他の装置と通信を行うための通信手段と、

電子機器間の通信が認証されることによって許可される複数の機器がグループ化されて登録されるグループ情報が記憶される記憶手段と、

上記複数の電子機器の通信開始前に上記ネットワークを通して送信する機器ＩＤと上記記憶手段に記憶されたグループ情報とに基づいて、電子機器間の通信が許可されているか否かを判別する判別手段と、

上記ネットワーク接続され送られる機器ＩＤに基づいて電子機器を特定して通信を交換処理する交換装置へ、上記判別結果

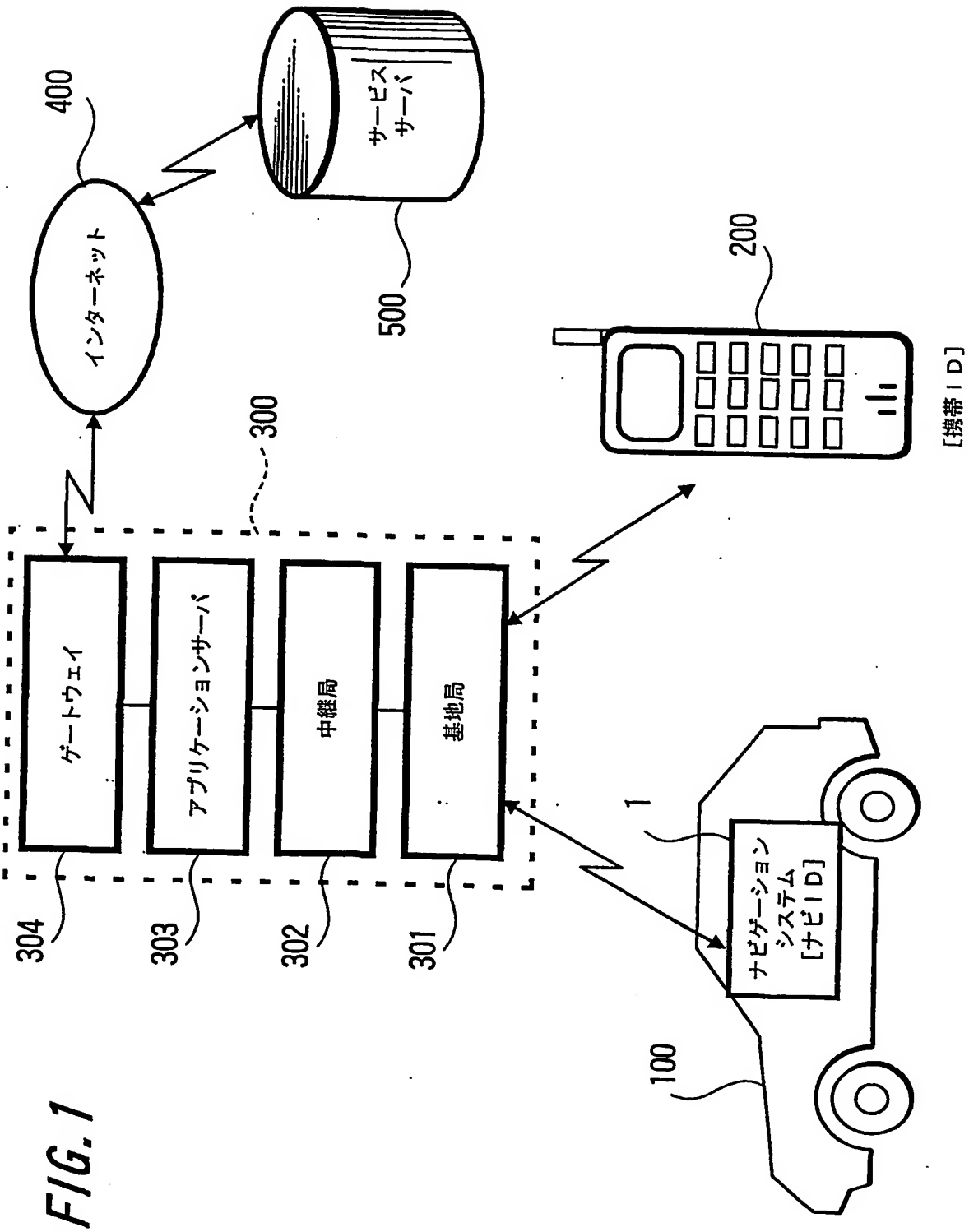

400
サービス
サーバ
インターネット
500
200
[携帯ＩＤ]
300
ゲートウェイ
アプリケーションサーバ
中継局
基地局
304
303
302
301
1
ナビゲーション
システム
[ナビＩＤ]
100

FIG. 1

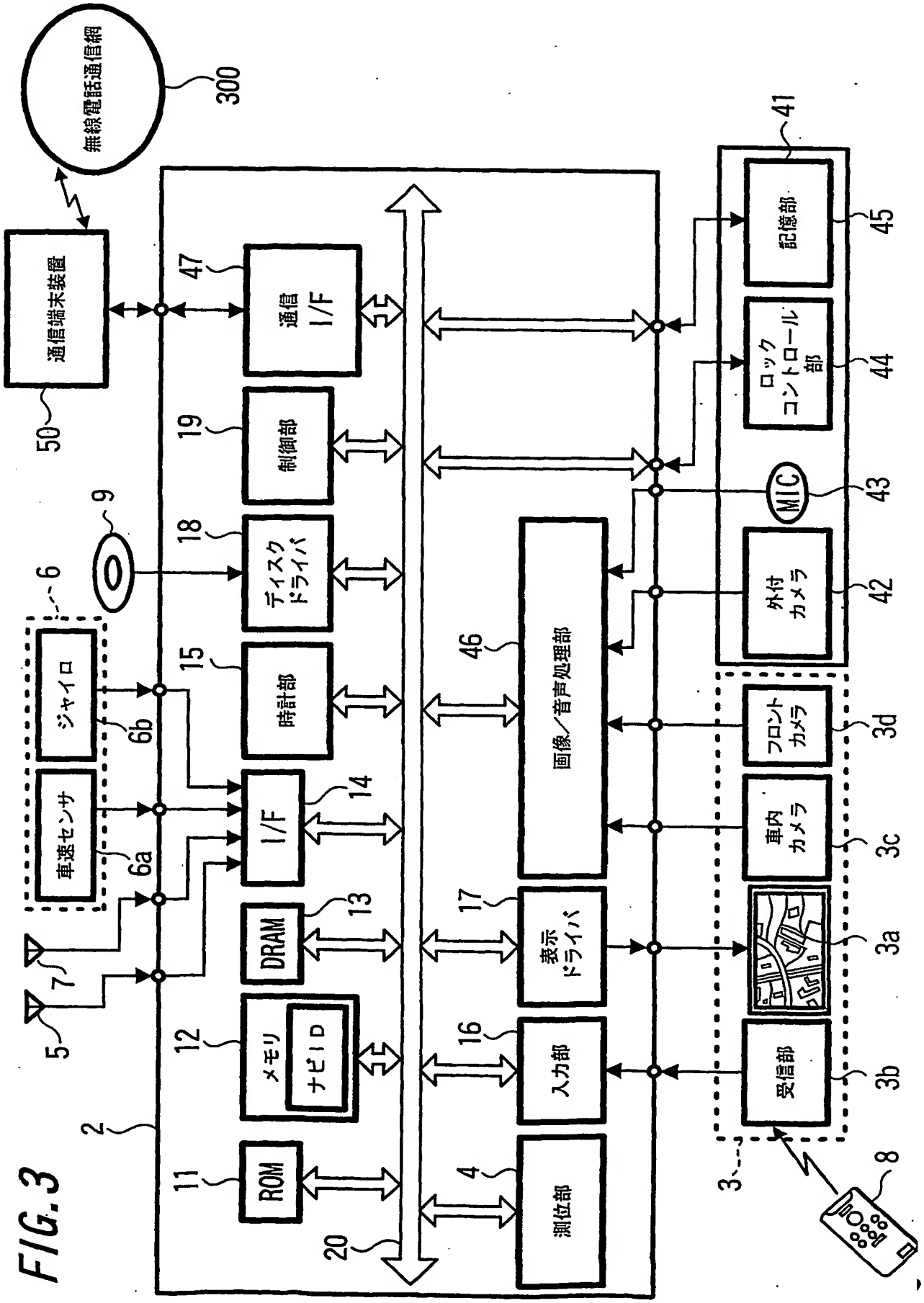
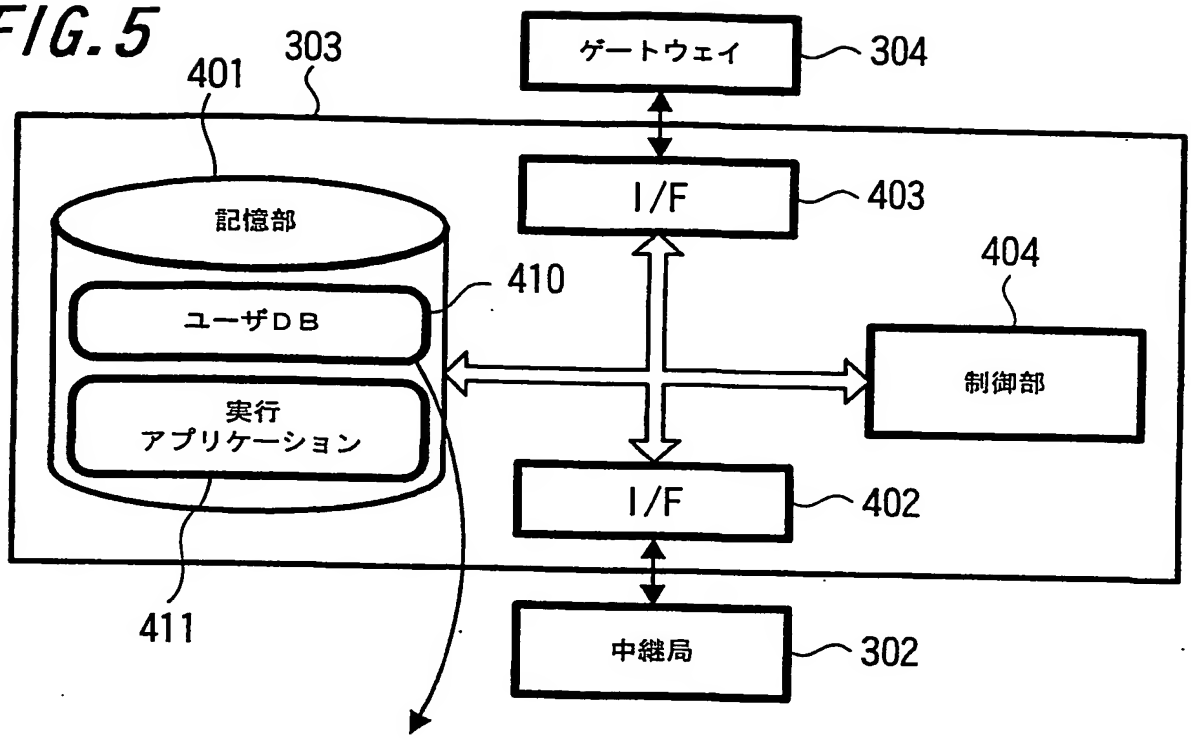

無線電話通信網
300
通信端末装置
50
通信 I/F
47
制御部
19
ディスク ドライバ
18
時計部
15
I/F
14
DRAM
13
メモリ
ナビID
12
ROM
11
測位部
4
入力部
16
表示 ドライバ
17
画像／音声処理部
46
ジャイロ
6b
車速センサ
6a
6
9
5
7
2
20
記憶部
45
ロック コントロール 部
44
MIC
43
外付 カメラ
42
フロント カメラ
3d
車内 カメラ
3c
3a
受信部
3b
3
8
41

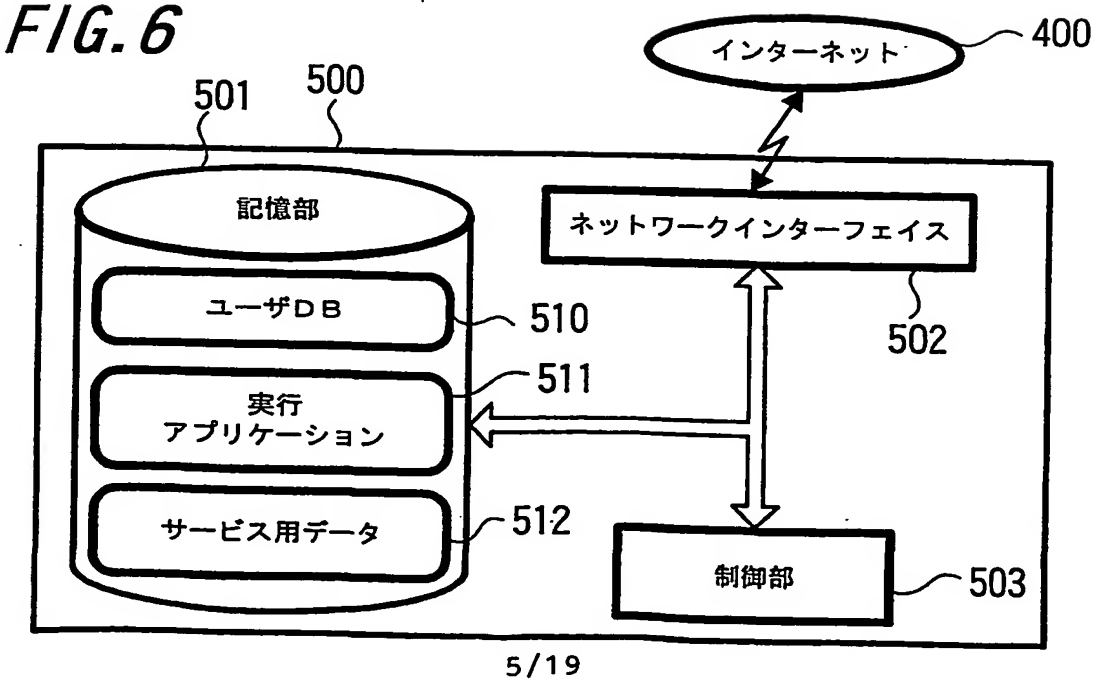
FIG. 3

FIG. 5



1	ユーザ情報	携帯ID（電話番号）	ナビID（電話番号）	パスワード
2				
3				

FIG. 6



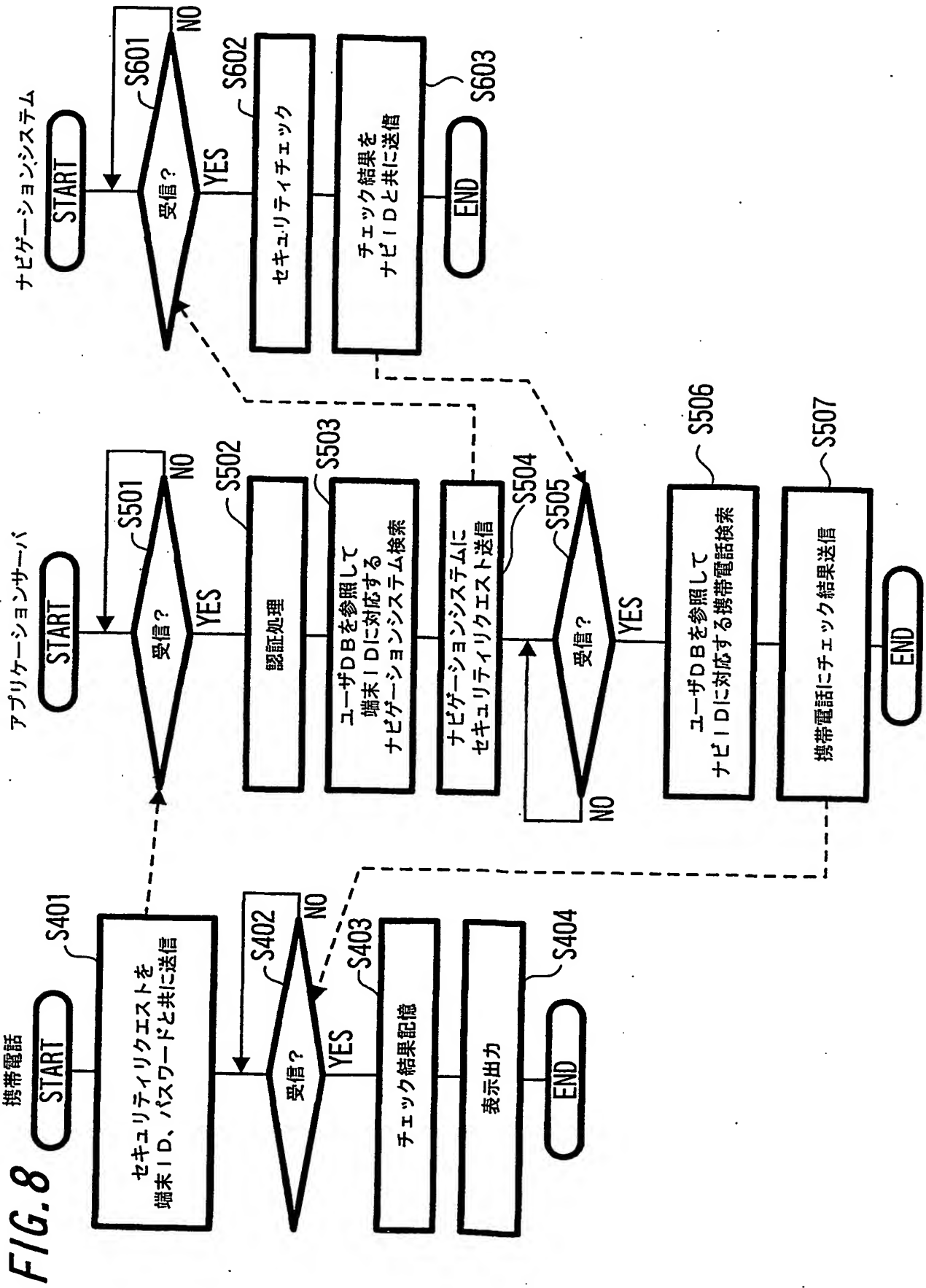
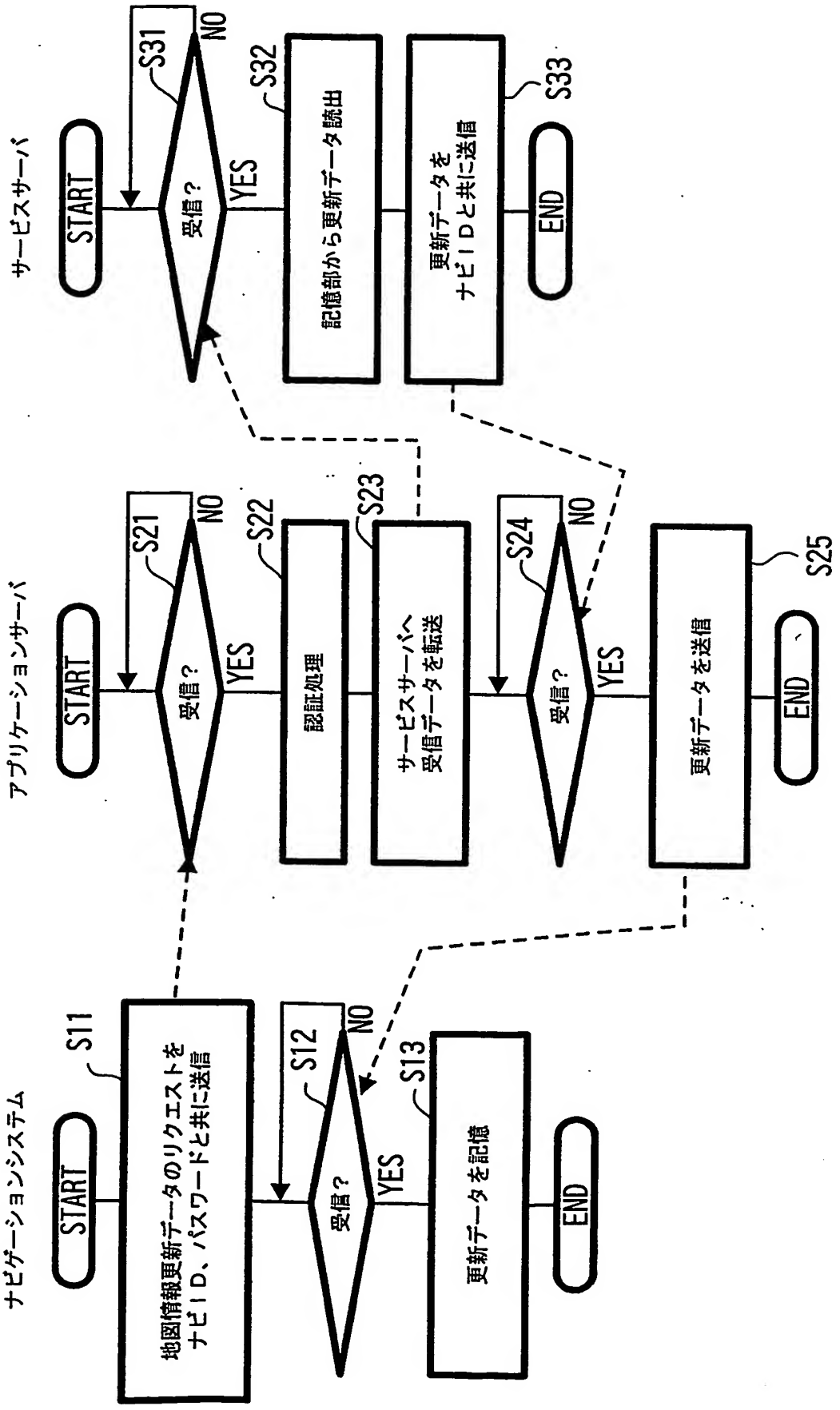

携帯電話
START
セキュリティリクエストを
端末ＩＤ、パスワードと共に送信
S401
受信？
NO
YES
S402
チェック結果記憶
S403
表示出力
S404
END
アプリケーションサーバ
START
受信？
NO
YES
S501
認証処理
S502
ユーザＤＢを参照して
端末ＩＤに対応する
ナビゲーションシステム検索
S503
ナビゲーションシステムに
セキュリティリクエスト送信
S504
受信？
NO
YES
S505
ユーザＤＢを参照して
ナビＩＤに対応する携帯電話検索
S506
携帯電話にチェック結果送信
S507
END
ナビゲーションシステム
START
受信？
NO
YES
S601
セキュリティチェック
S602
チェック結果を
ナビＩＤと共に送信
S603
END

FIG. 8

FIG. 10


ナビゲーションシステム
START
地図情報更新データのリクエストをナビID、パスワードと共に送信
S11
受信？
S12
NO
YES
更新データを記憶
S13
END
アプリケーションサーバ
START
受信？
S21
NO
YES
認証処理
S22
サービスサーバへ受信データを転送
S23
受信？
S24
NO
YES
更新データを送信
S25
END
サービスサーバ
START
受信？
S31
NO
YES
記憶部から更新データ読出
S32
更新データをナビIDと共に送信
S33
END

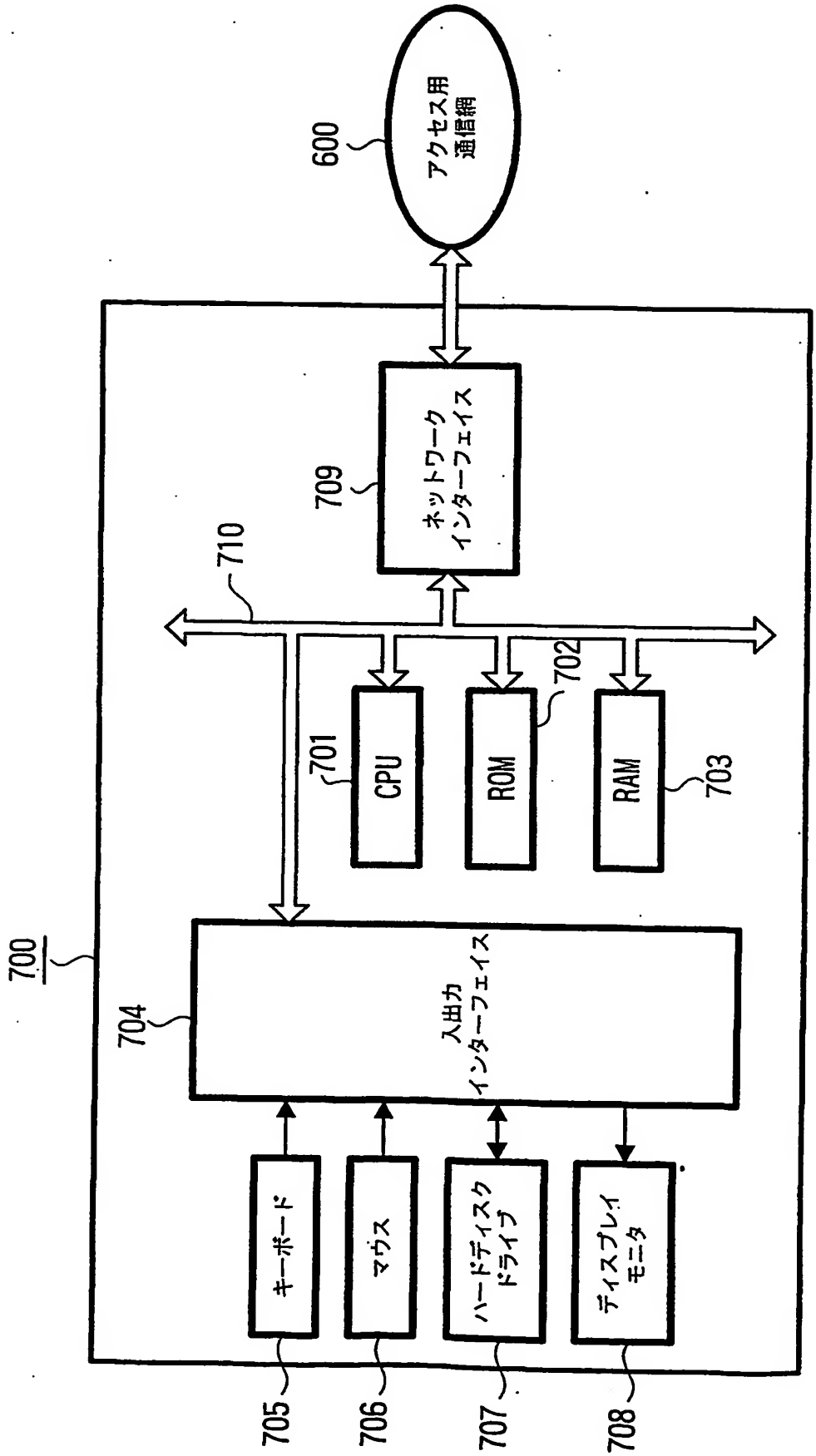

600
アクセス用
通信網
709
ネットワーク
インターフェイス
710
701
CPU
ROM
702
RAM
703
700
704
入出力
インターフェイス
キーボード
マウス
ハードディスク
ドライブ
ディスプレイ
モニタ
705
706
707
708

FIG. 12

FIG. 14

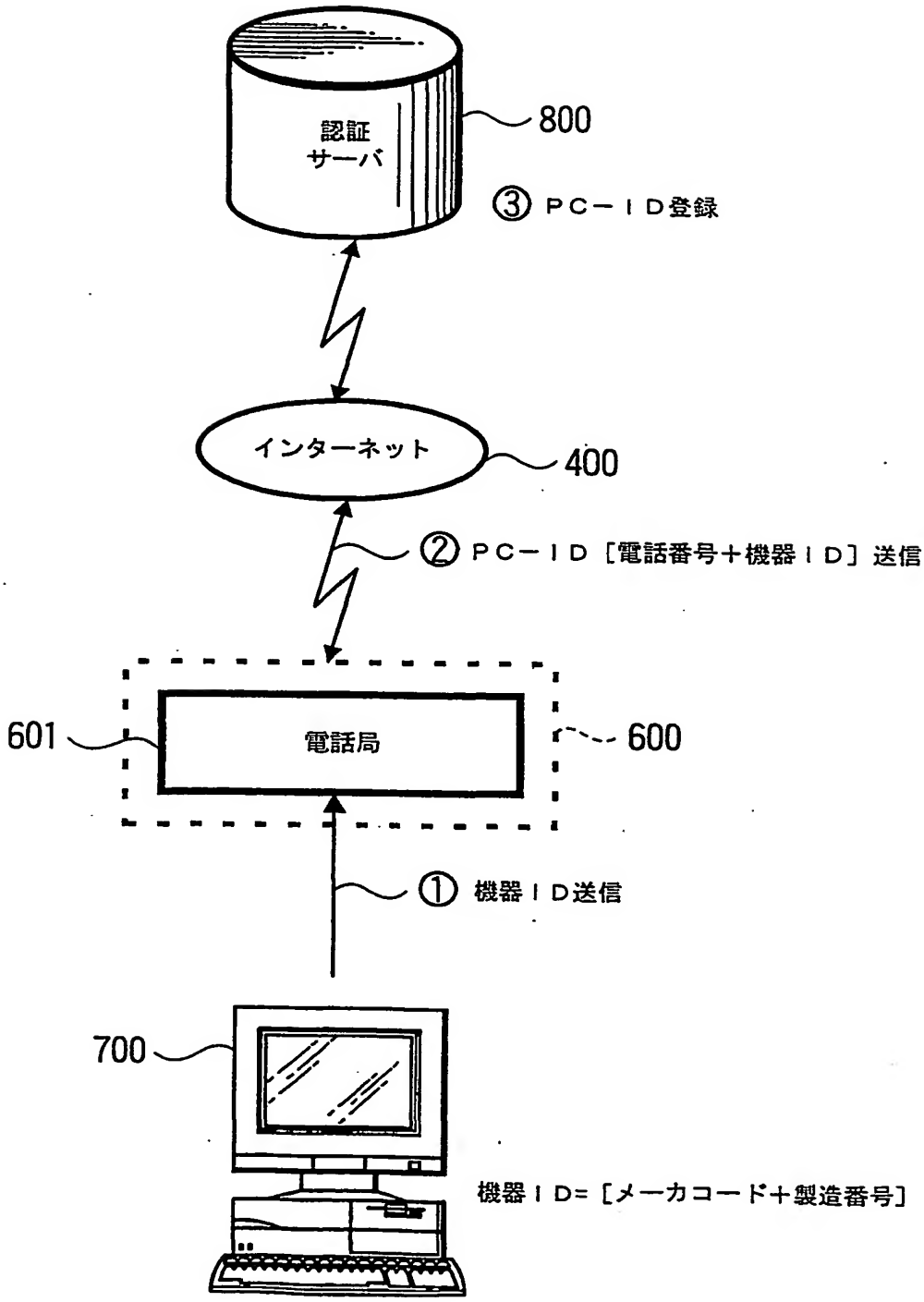
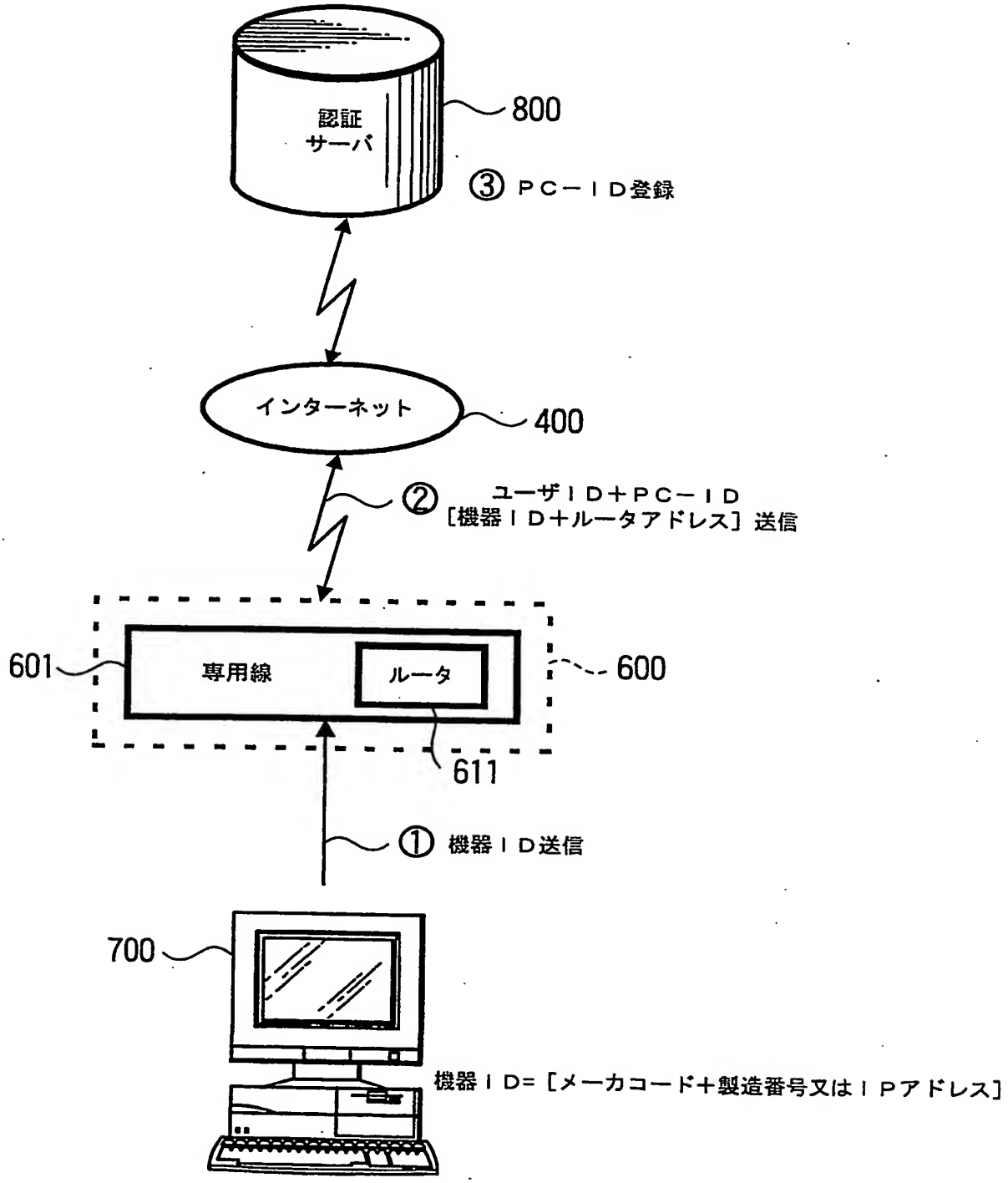

認証
サーバ
800
③ PC－ID登録
インターネット
400
② PC－ID［電話番号＋機器ID］送信
601
電話局
600
① 機器ID送信
700
機器ID=［メーカコード＋製造番号］

FIG. 16


認証
サーバ
800
③ ＰＣ－ＩＤ登録
インターネット
400
② ユーザＩＤ＋ＰＣ－ＩＤ
［機器ＩＤ＋ルータアドレス］送信
601
専用線
ルータ
600
611
① 機器ＩＤ送信
700
機器ＩＤ=［メーカコード＋製造番号又はＩＰアドレス］

符　号　の　説　明

1　ナビゲーションシステム、
2　ナビゲーション本体部、
3　ディスプレイモニタ部、
3 a　表示画面、
3 b　受信部、
3 c　車内カメラ、
3 d　フロントカメラ、
4　測位部、
8　リモートコントローラ、
8 a　緊急キー、
9　記録媒体、
1 1　ＲＯＭ、
1 2　メモリ、
1 3　ＤＲＡＭ、
1 4　インターフェイス、
1 5　時計部、
1 6　入力部、
1 7　表示ドライバ、
1 8　ディスクドライバ、
1 9　制御部、
2 0　バス、
4 1　セキュリティシステム部、
4 5　記憶部、
4 6　画像音声処理部、
4 7　通信インターフェイス、
5 0　通信端末装置、
2 0 0　携帯電話、

６００　アクセス用通信網、
７００　パーソナルコンピュータ、
７０１　ＣＰＵ、
７０２　ＲＯＭ、
７０３　ＲＡＭ、
７０４　入出力インターフェイス、
７０５　キーボード、
７０６　マウス、
７０７　ハードディスクドライブ、
７０８　ディスプレイモニタ、
７０９　ネットワークインターフェイス、
７１０　内部バス、
８００　認証サーバ、
８０１　記憶部、
８０２　ネットワークインターフェイス、
８０３　制御部、
８１０　認証用ユーザデータベース、
８１１　実行アプリケーション

国際調査報告

国際出願番号 PCT／JP01／05664

A. 発明の属する分野の分類（国際特許分類（IPC））

Int.Cl' G08G1/137, H04M11/00 302, H04M 3/42, G06F13/00 530, G06F17/60 326

B. 調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int.Cl' G08G1/137, H04M11/00 302, H04M 3/42, G06F13/00 530, G06F17/60 326

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1926-1996
日本国公開実用新案公報	1971-2001
日本国登録実用新案公報	1994-2001
日本国実用新案登録公報	1996-2001

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C. 関連すると認められる文献

引用文献のカテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 10-255022 A(ソニー株式会社), 25.9月.1998(25.09.98) 第5頁第8欄第36行－第6頁第9欄第21行、第1図(ファミリーなし)	1-16
Y	JP 11-260045 A(ソニー株式会社), 24.9月.1999(24.09.99) 第14頁第25欄第30行－同頁第26欄第25行、第10図(ファミリーなし)	1-16
Y	JP 10-336765 A(ソニー株式会社), 18.12月.1998(18.12.98) 特許請求の範囲の記載、(ファミリーなし)	6-16

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日 10.09.01	国際調査報告の発送日 18.09.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 仲村 靖 印 3H 9239 電話番号 03－3581－1101 内線 3314

様式PCT／ISA／210（第2ページ）（1998年7月）